Reset Form

✓

PSA JACKSONVILLE
SYSTEM ACCESS REQUEST

Name (Last, First, MI):	Rate/Rank/Grade:	PRD: (yy/mm)
Command:	Dept:	
Phone:	Email Address:	

1. Per PSAJAXSORM 5230-001, all PSA Jacksonville LAN/WAN users shall:

- Be limited to accessing only that data, controlled information and software for which they are authorized.
- Immediately report all security incidents and potential threats and vulnerabilities involving information systems to the command Network Security Officer (NSO)/Information Systems Security Manager (ISSM) at PSA via their local ISSO.
- Protect their authenticators (I.E. Passwords, login id) and report any compromise or suspected compromise of a password to the local ISSO. Password sharing is strictly prohibited.
- Be issued a password that consists of a minimum of 8 characters and will include a combination of mixed case, alphanumeric characters (i.e., PtyZ$efll or MwZXiuy13).
- Ensure that system media and systems output is properly classified, marked, controlled and stored.
- Protect Network workstations from unauthorized access (You shall lock **(Ctrl-Alt-Del)** or logout when not at workstation).
- Inform the local ISSO when access to the LAN is no longer required. (i.e. completion of project, PCS Trf, Retirement, etc).
- Use the NIPRNET/Internet only per PSAJAXSORM 5230-001.
- Not copy nor manually move data atxl files from a CLASSIFIED system to a lower level CLASSIFIED or UNCLASSIFIED system, unless the process is performed in accordance with authorized downgrade processes and procedures. Contact the Command ISSM prior to performing any of these procedures (i.e., Gate Guard and DMS {Defense Messaging System}) PCs.

2. Due to the need of safeguarding network information, hardware, firmware and software, users shall not attempt to:

- Introduce malicious code into the Command's Sensitive But Unclassified (SBU) LAN.
- Attempt to bypass, strain or test security mechanisms prescribed for a given network. If security mechanisms must be bypassed for any reason, users must coordinate the procedure with the command NSO or ISSM and receive written permission for the procedure.
- Introduce or use unauthorized software, firmware or hardware on the command's SBU networks, workstations or stand-alone systems.
- Violate software copyright and license restrictions.
- Assume the roles and privileges of others and attempt to gain access to information for which they have no authorization.
- Relocate LAN workstations, printers, scanners, without proper authorization from ISD personnel.

3. Use of Email. Please see PSAJAXSORM 5230-001(Internet and Email Policy). NOTE: A more restrictive OIC policy may apply.

4. I understand that if I knowingly make, acquire or use unauthorized copies of computer software, disclose unauthorized matters pertaining to CLASSIFIED, SENSITIVE UNCLASSIFIED and/or Privacy Act information, I may be subject to discipline according the circumstances under the UCMJ and applicable Federal and State laws.

5. I understand that software will only be used in accordance with the software licensing agreement.

6. I understand that pursuant to federal statue, illegal reproduction or use of commercial software is subject to civil damages up to $l00,000.00 (for willful infringement) and criminal penalties to include fines and imprisonment for multiple reproductions for commercial purposes or private financial gain. In accordance with Tide 17, United States Copyright Code, Section 504 and 506.

7. I understand that by signing this user agreement (expressed consent) and successfully logging onto a system (implied consent i.e. DOD warning banner) your activities are subject to monitoring. During monitoring, information may be examined, recorded, copied and used for authorized purposes without your prior knowledge.

I have read and understand this System Access Request and PSAJAXSORM 5230-001 (Internet and Email Policy) concerning user responsibilities for the PSA Jacksonville LAN/WAN and will abide by them.

Signature:

Date: